ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

July 13, 2000

COMMAND, CONTROL,
COMMUNICATIONS, AND
INTELLIGENCE

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: DoD Personnel Security Migration Program-Joint Personnel Adjudication System

In 1993, the Department mandated the implementation of DoD migration systems, data standards, and process improvements within the Military Departments and Defense Agencies in order to improve the quality, accuracy, and utility of DoD information while reducing the cost of DoD operations. In accordance with this mandate and since 1995, OASD(C3I) has led the effort to develop the Joint Personnel Adjudication System (JPAS) as DoD's personnel security migration system for "real time" clearance and access verification. JPAS will eliminate multiple, costly "stovepiped" clearance management systems, create a single, "virtual" consolidation of the DoD Central Adjudication Facilities (CAF) and will reach more than 30,000 security managers throughout the DoD Components and industry.

Recently, several key developments have further emphasized the need for all addressees to ensure expeditious migration to JPAS during FY01, down to the lowest level security manager. These include: 1) the ability to rapidly and accurately reflect the current classified accesses of cleared DoD personnel, including contractors; 2) the ability to accurately reflect the true size of the periodic reinvestigation backlog based on an individual's current access; 3) the need for comprehensive and timely security data required to help prioritize the submission of periodic reinvestigations; 4) a source of contractor clearance and personnel reliability data for the Common Access Card; 5) the need to capture and maintain relevant security data on personnel with access to DoD Critical Information Technology systems; and 6) the single focal point to provide TOP SECRET/SCI accesses for DoD personnel to the Central Intelligence Agency's forthcoming security clearance database. JPAS will also play a significant role in achieving resolution of a variety of other personnel security issues involving clearance/access reciprocity, duplication and accuracy of clearance data.

Critical to the JPAS application design was the selection of a system overview, which embraces current DoD information systems policy for: Defense Information Infrastructure/Common Operating Environment; Data Standardization; Public Key Infrastructure; Network Security; and the use of NETSCAPE. Therefore, with the assistance of the Defense Information Systems Agency and the DoD Deputy Chief Information Officer, a centralized database/centralized processing system architecture has been selected for JPAS. This system architecture will not only achieve the above objectives but will also facilitate transition to a components-based architecture as interfaces between JPAS and external organizations mature. Further, JPAS incorporates additional DoD goals such as business process re-engineering; use of NIPRNET technology; virtual consolidation of DoD CAFs; and an efficient use of personnel security information system fiscal resources. This system architecture results in a net savings of $18.8M to the DoD over the FYDP. This does not include the significant savings which will accrue to DoD and industry through the ability to more rapidly and efficiently put people to work with the necessary security clearance or access.

Attached is a brief description of JPAS and the minimum hardware requirements for security managers/special security officers that will be required to use the system (Attachment 1). In the near future, this office will release more detailed information regarding the requirements to access JPAS, such as, internet protocol ports, network security, and training.

The continuing security and resource challenges within DoD support the initial beta testing of JPAS between September 30, 2000 and January 31, 2001, in order to maximize efficiencies and provide rapid and real-time security clearance support to the warfighter. Your support of this initiative is encouraged. Please ensure the widest possible dissemination of this memorandum within your component. Frequently asked questions regarding JPAS are also attached at Attachment 2. Additional information regarding JPAS may be accessed at the web site, http://162.24.112.4/, or from the JPAS Program Management Office at Bolling Air Force Base, 202-767-4901/4886 (DSN 297). The C3I point of contact for JPAS is Mr. Peter Nelson, 703-697-3969.

Arthur L. Money

Attachments

JOINT PERSONNEL ADJUDICATION SYSTEM (JPAS) DESCRIPTION

JPAS is the Department of Defense (DoD) personnel security migration system for the DoD CAFs and DoD personnel security managers for non-SCI and SCI programs. It represents the virtual consolidation of the nine DoD CAFs using a centralized database with centralized computer processing. The two applications supporting JPAS are: the Joint Adjudication Management System (JAMS) for the DoD CAFs only and the Joint Clearance and Access Verification System (JCAVS) for approximately 30,000 CAF customers, including Defense industry. Telecommunications and automated information systems interfaces will serve as the cornerstone for the CAFs' virtual consolidation and ensure standardization and re-engineering of core personnel security and adjudication processes.

To date, DoD has expended more than $12M in fiscal resources for JPAS business process re-engineering, data standardization, software development, integration, and software/software license purchases.

JPAS MINIMUM HARDWARE REQUIREMENTS

Pentium Computer, minimum 133mhz with 128 MB RAM
NETSCAPE Browser (4.x) **DoD Mandate
NIPRNET Access

Attachment 1

FREQUENTLY ASKED QUESTIONS ABOUT JPAS

1. What is the Joint Personnel Adjudication System (JPAS)?

JPAS is the Department of Defense (DoD) personnel security migration system for: 1) the virtual consolidation of the DoD Central Adjudication Facilities (CAFs); 2) use by non-SCI security program managers; 3) Special Security Officers; 4) Special Access Program (SAP) program managers; and in the future 5) DoD contractor Facility Security officers (future), in order to assist them in the ability to obtain real-time, up to date, accurate, clearance and access information on cleared DoD personnel as well as to automate the unit level personnel security management. JPAS will be the single, authoritative DoD source of clearance and access information upon which DoD users will be able grant immediate access to classified information. JPAS will use a centralized database with centralized computer processing and application programs for standardized DoD personnel security processes. JPAS automates both core and CAF-unique functionality and provides "real-time" information regarding clearance, access and investigative status to authorized DoD security personnel and other interfacing organizations, such as Defense Security Service (DSS), Defense Manpower Data Center (DMDC), Defense Civilian Personnel Data System, Office of Personnel Management, and Air Force Personnel Center. Interfaces with the Navy and Army military personnel systems will be accomplished through the Defense Eligibility and Enrollment System (DEERS) at DMDC pending the successful implementation of the single, unified military personnel system, which is currently under development. Telecommunications and automated information systems interface software will serve as the cornerstone for the CAFs virtual consolidation and ensure re-engineering of core personnel security and adjudication processes.

2. What applications support JPAS?

There are two applications in JPAS to support both the adjudication process and the unit personnel security management process. The adjudication application is known as the Joint Adjudication Management System (JAMS) and will be available only for adjudicative personnel assigned to one of the nine DoD CAFs. The unit personnel security management application is known as the Joint Clearance and Access Verification System (JCAVS) and will be available for all DoD non-SCI and SCI security managers, entry control personnel, key personnel organizations, and other entities as approved by the JPAS Executive Steering Committee/Configuration Management Board.

3. Who determines the access authorizations for JPAS?

Each Military Department and DoD Agency will determine the specific JPAS customer user base for their respective component or Agency. The policy representatives for the component or agency will establish the designation of this office/organization as the focal point. In release one of JPAS, contractor security personnel will not be authorized access to JPAS; however, contractor access is planned for a future release in about September 2001. The intent is to make JPAS available to the lowest level DoD organizational unit (est 30,000) in order to support timely and accurate personnel security access decisions.

4. What are the software and hardware requirements for JPAS?

Each JPAS user will be required to have a Pentium computer, 133 MHz (minimum), 128 MB RAM with NETSCAPE 4.X (current DoD version), and a Public Key Infrastructure (PKI) certificate/token (Final determination pending). JPAS is a web-based application and all users must be able to access JPAS via "port 443" at the installation firewall.

5. What are the advantages to using a centralized database with centralized processing architecture?

- Implements DoD Public Key Infrastructure (PKI) policy, using X.509v3 certificates.
- Implements the DoD mandate to use NETSCAPE as the DoD Web Browser.
- Encrypts transmission between JPAS and external interfacing systems.
- Meets DII COE, I&RTS level 6 compliant.
- Mandates DoD Joint Technical Architecture (JTA) Information Systems Security Standards.
- Implements DoD Directive 5200.28 (Security Requirements for Automated Information Systems). Data in JPAS shall be considered as sensitive unclassified information and thus shall be protected with minimum class C2 security as prescribed in 5200.28.
- No additional hardware requirements associated with the CAFs such as the purchase of servers; no requirement for a complete conversion of hardware suites. Pentium computers purchased to achieve interoperability with the DSS Case Control Management System may be used; however, CAF life-cycle replacements are on going.
- Mandates DoD data standardization and configuration control.
- Reduces cost of database software licenses to support a network enterprise license for users of JPAS within DoD.
- Facilitates both legacy and migration system external interfaces (Defense Security Service, Defense Manpower Data Center, Defense Civilian Personnel Data System, Office of Personnel Management, and Air Force Personnel Center).

6. What are the JPAS Timelines?

JPAS will begin BETA testing 30 Sep 00, with 46 participating organizations. These organizations represent the Military Departments and DoD Agencies in the CONUS and Overseas. The specific JPAS timeframe is as follows:

11-15 Sep 00 – BETA test Training
30 Sep 00 – BETA test begins
30 Jan 01 – BETA test ends
6-8 Feb 01 – JPAS Workshop (Policy Representatives, JAMS/JCAVS Users)
20 Feb 01 – CAF/Unified Command Implementation
12 Mar 01 – Department of Navy/DoD Agencies
22 Apr 01 – Department of Army/DoD Agencies
4 Jun 01 – Department of Air Force/DoD Agencies
23 Sep 01 – Defense Industry phase-in
30 Sep 01 – CAF Stovepipes begin phase-out

7. How will JPAS users be trained? When?

JPAS will use the "train-the-trainer" concept. Adjudicator training will be accomplished in the National Capital Region at several of the DoD CAFs, primarily, Army, Navy, and AF beginning Jan 01. Security Managers and Special Security Officers will be trained beginning in Jan 01 at training sessions hosted by the Unified Commands. For example, US Central Command will host a training session for personnel within a 100-150 mile radius of McDill AFB. Several host training sites have been requested and identified, however, additional sites are needed and actions are underway with the MILDEPs to accomplish. Additionally, JPAS training will be accomplished via the DIA Security Officer Mobile Course and the DSS Academy throughout 2001 and 2002.

Attachment 2